UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

THE UNITED STATES OF AMERICA, Plaintiff, -against- ROMAN STORM, ET AL., Defendant.	Case No. 23 Cr. 430 (KPF) Oral Argument: July 12, 2024

REPLY IN SUPPORT OF ROMAN STORM'S MOTION TO DISMISS

Brian E. Klein
Keri Curtis Axel
Kevin M. Casey
Waymaker LLP
515 S. Flower Street, Suite 3500
Los Angeles, California 90071
(424) 652-7800

Attorneys for Roman Storm

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes and Regulations

Rules

Miscellaneous

I. PRELIMINARY STATEMENT

The Indictment of Mr. Storm does not survive the government's admissions in its own opposition brief. The government admits that Mr. Storm did not violate any laws when he participated in developing an agnostic software tool, the Tornado Cash software, and made it publicly available. Moreover, the government admits that Mr. Storm did not have any agreement with the criminals who allegedly misused Tornado Cash to transmit and launder money and to evade sanctions. In fact, by the time criminals allegedly began misusing it, the Tornado Cash protocol was, as the government concedes, immutable and available to anyone with an Internet connection.

In support of Count Two, the alleged conspiracy to operate an unlicensed money transmitting business in violation of 18 U.S.C. § 1960, the government argues that the statute does not require any element of control over the money being transmitted, contrary to both the statutory language and longstanding regulatory guidance. The government overlooks that Tornado Cash is simply a software tool that allows *users* to transact privately on the blockchain. Crucially, the government acknowledges that Mr. Storm and the Peppersec developers did not charge any fees for Tornado Cash transactions. Instead, it argues that third-party relayers charged fees for Tornado Cash transactions but fails to acknowledge that the use of relayers, as well as the fees charged by them, was optional. The government's expansive interpretation would effectively ban anonymizing software and chill technological development.

Count One fails for the same reason. There was no financial transaction by a financial institution, as required by 18 U.S.C. § 1956(c)(4)(B), because Tornado Cash is not a financial institution. The government's attempt to rescue Count One with an alternative definition of financial transaction fails because the Indictment lacks any allegation that Mr. Storm and the

Peppersec developers "conduct[ed]" any such "transaction," knowing it contained illegal proceeds. The government contends that Mr. Storm had an "agreement" with other Peppersec developers but admits it was to develop software and was not between Mr. Storm and any alleged bad actor. Count One also implicitly seeks to convict Mr. Storm on an impermissible negligence theory, but this does not satisfy money laundering's specific intent requirement.

Count Three is the final, failed attempt to make the government's "conspiracy theory" stick, this time alleging sanctions evasion in violation of the IEEPA. The government relies on an obscure OFAC regulation it claims overrides the longstanding constitutional and statutory protections for informational materials, including software. The government also argues that "willfulness" is established because, years after Mr. Storm helped develop the Tornado Cash software, he purportedly "deliberately chose an ineffective remedy" when Tornado Cash was allegedly misused by criminal hackers. Somehow, the government believes that if software developers do not do enough to combat cybercrime, they are criminally liable under the IEEPA. No court has ever approved these misguided theories.

The Court should not indulge the government's prosecutorial overreach. The government's dislike of non-public transfers of cryptocurrency does not allow it to engage in unconstitutional regulation by enforcement. The government repeatedly begs for a trial, but a trial is not permitted where, as here, the Indictment is patently deficient. Dismissing the Indictment would not extend blanket immunity to software developers, as the government contends, but would instead conform with existing law and prevent a serious erosion of legal and constitutional safeguards. Mr. Storm's motion to dismiss should be granted.

II. ARGUMENT

The Indictment should be dismissed pursuant to Rule 12 for failure to state offenses. The government claims that Mr. Storm is trying to rely on disputed facts in support of his motion to dismiss. (Dkt. 53, Gov't Opposition ("Opp.") at 4.) Not true. The government does not dispute the critical facts that support each of Mr. Storm's arguments for dismissal. In fact, three core admissions defeat the government's case and merit dismissal of the Indictment.

First, the government claims that Tornado Cash was a business, but it concedes that the "business" had the legitimate goal of enhancing privacy for transactions on the blockchain (*see* Opp. at 9, 71); it explicitly admits the legality of Tornado Cash (*id.* at 31), and that American citizens have lawfully used Tornado Cash (*id.* at 58). The government's second fatal admission is that the alleged criminal misuse occurred *after* Tornado Cash had become immutable and publicly available on the Internet in May 2020, at which point the government admits Mr. Storm "no longer exercised control over the Tornado Cash pools" (*id*. at 13), but that is before any alleged conspiracy began. (*See id.* at 43.) Third, the government admits that Mr. Storm did not commit any of the unlawful transactions allegedly processed by Tornado Cash and that he did not have any agreement with the criminals who allegedly did. (*Id.* at 40, 46.)

These fatal admissions mean the core of the "conspiracy theory" against Mr. Storm is the government's belief that he should have done more to stop criminal hackers from misusing Tornado Cash. (*See, e.g.*, Opp. at 15.) This theory is not supported by any of the statutes the Indictment charges Mr. Storm with violating, and it violates fundamental Constitutional protections.

A. Count Two, the Conspiracy to Operate an Unlicensed Money Transmitting Business Charge, Should Be Dismissed

To meet the elements of Count Two, the government is required to allege control over the funds and that the business charged a fee for making transfers. The government does not dispute the essential facts showing defendants' lack of control over the funds; for example, the government notes that "the Tornado Cash service did not typically maintain a copy of the secret note" (Opp. at 10) and agrees that the Tornado Cash pools were immutable during the relevant time period and not under Mr. Storm's control. (*Id.* at 8, 13.) Likewise, there is no dispute that neither Tornado Cash nor Mr. Storm and the Peppersec developers charged a fee for transactions. (*Id.* at 36.) All that is left for the Court to decide is a question of law: whether money transmitters must control the funds they transfer and charge fees. Because Tornado Cash does not control any funds or charge fees, it is not a money transmitting business.

1. Control Is an Essential Part of a Money Transmitting Business

The government challenges Mr. Storm's contention that control over the funds is necessary to be a money transmitting business. (*See* Opp. at 24-31.) Primarily, the government complains that the word "control" does not appear in the statutes. (*Id.* at 29-30.) But the Court must interpret the words that *do* appear in the statutes, "transmit," "transfer," and "accept," and each requires control. *See* 18 U.S.C. § 1960(b)(2); 31 U.S.C § 5330(d)(2) & (d)(1)(A).[1]

[1] The government disagrees that the definition of money transmitting business in Section 1960 is coextensive with that in 31 U.S.C. § 5330. (Opp. at 19 n.4.) Yet, the government acknowledges, as it must, that the definitions necessarily merge with respect to a violation of 18 U.S.C. § 1960(b)(1)(B) because that subsection requires a violation of the registration requirement of 31 U.S.C. § 5330. The government nevertheless claims that the same definition of money transmitting should not apply with respect to a violation of 18 U.S.C. § 1960(b)(1)(C). Money transmitting cannot mean one thing for one subsection of the statute but something else for a different subsection of the same statute. *See United States v. Santos*, 553 U.S. 507, 522 (2008) ("the same word, in the same statutory provision," cannot have "different meanings in different factual contexts"). Indeed, in *United States v. E-Gold, Ltd.*, 550 F. Supp. 2d 82, 92 n.10 (D.D.C. 2008), cited by the government, the court expressly acknowledged that "there is virtually no

The government's argument that a "transfer" can be effected without control proves the point. (*See* Opp. at 24-25.) The government contends that a USB cable "transfers" data, and a frying pan "transfers" heat. (Opp at 24.) But these examples prove nothing, except perhaps that the government believes it could indict a frying pan—or that the developer of a USB cable could be charged with operating an unlicensed money transmitting business if someone else used that cable to transfer funds. That cannot be what Congress intended in a criminal statute.

Indeed, that is the fundamental problem with Count Two. Tornado Cash is an inanimate—indeed, intangible—tool. It is the *users*—who have control over the funds—who make the transfers. Tornado Cash is just the software tool they use to do so privately—a tool that became immutable in 2020, as the Indictment acknowledges. (*See* Ind. ¶ 26.)

Dictionary definitions of transmit[2] and transfer[3] support this point because they involve taking an action, such as "conveying" or "causing" to pass, not merely the movement of data. (*See* Dkt. 37-1, Corrected Memorandum of Law in Support of Motion to Dismiss ("MTD") at 21.) The Black's Law Dictionary's definition of "funds transfer" further supports the point. (*See* Opp. at 25.) That definition includes "payment,"[4] defined as the "[p]erformance of an obligation by the delivery of money or some other valuable thing accepted in partial or full discharge of the

---

substantive difference, nor did Congress intend there to be a substantive difference, between the terms 'money transmitting' in Section 1960 and 'money transmitting business' in Section 5330."

[2] *Transmit*, Black's Law Dictionary (11th Ed. 2019); *see also* Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/transmit ("to send or convey from one person or place to another").

[3] *Transfer*, Merriam-Webster Dictionary Online, available at https://www.merriam-webster.com/dictionary/transfer ("to convey from one person, place, or situation to another" or "to cause to pass from one to another").

[4] *Funds Transfer*, Black's Law Dictionary (11th Ed. 2019).

obligation."[5] Again, the dictionary definition indicates an action—the performance of an obligation—not merely the physical or technological means of transferring funds.[6]

The government does not dispute that the term "accept," as used in Section 5330, is defined to mean "receive"[7] but notes alternative definitions of "to be able or designed to take or hold" and "to give admittance or approval to." (Opp. at 27-28.) Yet, "to take or hold" connotes control, as does "receive." And "to give admittance or approval to" is a different meaning of "accept" altogether, one that applies to things such as college acceptance, or acceptance into a social club—concepts that are inapplicable to a statute focused on money transmission.

The government also erroneously suggests that the language of the Second Circuit's opinion in *United States v. Velastegui,* 199 F.3d 590, 592 (2d Cir. 1999), that a "money transmitting business receives money from a customer and then, for a fee paid by the customer, transmits that money to a recipient" can be ignored as "dicta." (Opp. at 26-27.) First, the defendant in *Velastegui* argued that his conduct did not fall within Section 1960's ambit, so the Second Circuit's determination of what constitutes a money transmitting business under Section 1960 was essential to its decision and not dicta. Moreover, the Second Circuit subsequently re-affirmed this language in *United States v. Banki,* 685 F.3d 99, 114 (2d Cir. 2012). The case the

[5] *Payment*, Black's Law Dictionary (11th Ed. 2019).

[6] The government points out that Section 1960 uses the phrase "by any and all means." (Opp. at 25.) Mr. Storm does not contest that a transfer made via the Internet is a transfer. The point is that the person or entity making that transfer must have control over the asset being transferred, and Tornado Cash (and Mr. Storm and the Peppersec developers) did not.

[7] *See Accept*, Merriam-Webster Dictionary Online, available at https://www.merriam-webster.com/dictionary/accept ("to receive (something offered) willingly").The government asks this Court to ignore the interpretations of "receive" in *United States v. Stanley*, 896 F.2d 450, 451 (10th Cir. 1990), and *United States v. Dobbs*, 629 F.3d 1199, 1203–04 (10th Cir. 2011), holding that the term includes taking control of the item. (Opp. at 27 n.8.) It contends that these cases involve a "very different criminal statute," but the government provides no reason why the statutory context suggests a different meaning in Section 1960. (*See* Opp. at 27 n.8.)

government relies on, *United States v. Neumann*, No. 21 Cr. 439, 2022 WL 3445820, *6 (S.D.N.Y. 2022), is an unpublished district court decision, and its discussion of *Velastegui* is itself dicta because it relied on the defendant's concession as to a portion of the definition in Section 5330.[8]

Ultimately, the government acknowledges, as it must, that "in many or most cases, a money transmitter will take control of the funds that it is transmitting."[9] (Opp. at 29.) Yet, it offers no explanation as to why the statute should be stretched to include scenarios that are beyond the scope of what Congress anticipated. To so expand the statute's reach runs afoul of due process, the rule of lenity and the rule against novel constructions. (*See infra*, Section II.E.)

Indeed, the government fails to identify a single real example of a money transmitting business that does not take control of the funds being transmitted, other than its assertion that Tornado Cash is such a business. Instead, it offers up only a hypothetical business that accepts cash parcels in locked boxes to which it does not have the keys. (Opp. at 30.) But even in that

[8] The government also makes no effort to address the cases cited in Blockchain Association's amicus brief suggesting no Section 1960 liability when a defendant lacked control over the underlying value. *See United States v. $1,370,851.62 in U.S. Currency*, No. 09-21277-CIV-KING/BANDSTRRA, 2010 WL 11650916, at *6 (S.D. Fla. 2010) (no Section 1960 liability because defendant "did not *first* receive money from its clients"); *Givelify, LLC v. Department of Banking & Securities,* 210 A.3d 393, 401-02 (Pa. Commw. Ct. 2019) (petitioner did not "transmit[] money" because he did not "obtain" the money nor was the money "deposited into an account directly owned or controlled by [him]").

[9] Another case relied upon by the government, *United States v. Faiella,* 39 F. Supp. 3d 544 (S.D.N.Y. 2014) (Opp. at 21), supports the point that control is an essential part of being a "money transmitter." There, the government alleged that "Faiella received cash deposits from his customers and then, after exchanging them for Bitcoins, transferred those funds to the customers' accounts on Silk Road." *Id.* at 546. The government also alleged that "[t]hese were, in essence, transfers to a third-party agent, Silk Road, for Silk Road users did not have full control over the Bitcoins transferred into their accounts. Rather, Silk Road administrators could block or seize user funds." *Id.* Thus, the government effectively conceded that control was paramount to a finding of being a money transmitter, and the district court found that "in sending his customers' funds to Silk Road, Faiella 'transferred' them to others for a profit." *Id.*

scenario, the business would be able to direct the box and therefore arguably *does* have control over the funds in a way that Tornado Cash does not. Moreover, this example is much like certain armored car services that FinCEN has excluded from the definition of a money transmitter. *See* FinCen Guidance, FIN-2019-G001, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (May 9, 2019) ("Guidance") at 9.

The regulations issued by FinCEN are consistent and support the point that control is central to classification as a money transmitter. The regulations exclude from the definition of a "money transmitter" a person that only "[p]rovides the delivery, communication, or network access services used by a money transmitter to support money transmission services." 31 C.F.R. § 1010.100(ff)(5)(ii)(A). That is exactly what Tornado Cash does.[10]

The government cites no authority for the argument that this so-called "network access services" exemption applies only to an Internet service provider. (Opp. at 34-35.) The only case it relies on is a 2007 bankruptcy court case, *In re WorldCom, Inc.*, 371 B.R. 19, 23 (Bankr. S.D.N.Y. 2007). (*See* Opp. at 34.) That case, however, did not deal with the regulation here or have anything to do with money transmitters.[11] The Guidance makes clear that this exception applies more broadly to "suppliers of tools," including of anonymizing software that may be utilized in money transmission. Guidance at 20.[12]

---

[10] The government contends that even if Mr. Storm's conduct did fall under that exception, that would only affect the charged offense under subsection (b)(1)(B). (Opp at 34.) As noted above, the government's proposed interpretation that money transmitting can mean one thing for purposes of subsection (b)(1)(B) and another for subsection (b)(1)(C) should be rejected.

[11] It was also subsequently reversed by the district court, which the government failed to note. *In re WorldCom, Inc.,* Nos. 02-13533 (AJG), 07-cv-7414 (BSJ), 08-cv-3070 (BSJ), 2009 WL 2432370 (S.D.N.Y. 2009).

[12] The government also cites the regulations' second definition of "money transmitter" as any "other person engaged in the transfer of funds," citing 31 C.F.R. § 1010.100(ff)(5)(i)(A)-(B). (Opp. at 20.) This definition also uses the word "transfer," which requires control. Moreover, this definition would not apply to Tornado Cash because the term "funds" does not include

The government points out that control over the value is just one of the four factors the Guidance identifies for regulatory treatment of intermediaries as money transmitters: "(a) who owns the value; (b) where the value is stored; (c) whether the owner interacts directly with the payment system where the CVC [convertible virtual currency] runs; and (d) whether the person acting as intermediary has total independent control over the value." (Opp. at 32 (citing Guidance at 15).) But the list of factors is conjunctive, not disjunctive. Moreover, the other factors show that Tornado Cash is not a money transmitting business. Tornado Cash does not own the value, the value is stored on the blockchain, and the owner interacts directly with the protocol.

The government similarly argues, with respect to the Guidance provision discussing multi-signature wallet providers, that exercising "total independent control" is only one of three ways in which a provider may be treated as a money transmitter. (Opp. at 33 (quoting Guidance at 17).) This claim ignores the first sentence of that paragraph, which states: "If the multiple-signature wallet provider restricts its role to creating un-hosted wallets that require adding a second authorization key to the wallet owner's private key in order to validate and complete transactions, the provider is not a money transmitter because it does not accept and transmit value." (Guidance at 17.) This makes clear the test for a multi-sig wallet also turns on control (as it must, as the Guidance cannot and does not change the statutory and regulatory requirement of control). The second and third sentences are merely examples where such control might not exist, and none are applicable here, as the Tornado Cash protocol keeps no account records and

---

cryptocurrency. FinCEN Guidance FIN-2013-G001: *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* at 5, n.18 (Mar. 18, 2013).

has no account holders (*c.f. id.* at 8, 15), and the cryptocurrency owner interacts with the payment system directly.

The government tries to avoid the clear import of the Guidance by claiming that Tornado Cash is not a "wallet provider" (*see* Opp. at 21, 31-32), but even if the government's preferred characterization of Tornado Cash as a "mixing service" were adopted, Tornado Cash would not be treated as a money transmitting business under the Guidance. Notably, the Guidance explains that an "anonymizing software provider" is not a money transmitter because "suppliers of tools (communications, hardware, or software)" are "engaged in trade and not money transmission." Guidance at 20. The government claims that Tornado Cash is instead an "anonymizing service provider" (Opp. at 32), but this is incorrect because it does not "accept" the funds or "transmit" them to the recipient. *See* Guidance at 19 (an anonymizing service provider "accepts value from the customer and transmits" the value to the recipient).

Finally, the government retreats into discounting the Guidance as having "no authoritative effect." (Opp. at 33.) But the industry was entitled to rely on the Guidance regardless of whether the government characterized it as having authoritative effect. *See PHH Corp. v. CFPB,* 839 F.3d 1, 48 (D.C. Cir. 2016), *opinion reinstated in relevant part,* 881 F.3d 75 (D.C. Cir. 2018) (*en banc*). FinCEN cannot ignore its own current regulations on the network access exception or adopt new regulatory definitions of what it means to be a money transmitter without effecting those changes through notice and comment. (Dkt. 45, Amicus Br. of Block Chain Association ("BA Amicus Br.") at 17-18.) To impose criminal liability, in disregard of FinCEN's longstanding regulations and guidance would also deprive Mr. Storm and the public of due process and fair notice of what the law requires and violate the rule of lenity and the rule against novel constructions. (*See infra,* Section II.E.)

2. Tornado Cash Is Not a Money Transmitting Business Because It Did Not Charge a Fee

A second and independent reason Tornado Cash cannot be characterized as a money transmitting business is that it did not charge a fee for transmitting funds. The government nevertheless contends that Tornado Cash is a "business" because its developers profited from its operation. (Opp. at 35-36.) Tornado Cash is a software tool that users may utilize to transact privately on the blockchain. Thus, it is not a business, much less a money transmitting business.

Moreover, whether profits accrued to Mr. Storm or Peppersec is not the relevant inquiry. (*See* Opp. at 35.) It is perfectly permissible to profit from protected speech, and nothing about making profits transforms a software provider into a money transmitting business. Rather, the Second Circuit has made clear that a money transmitting business is one that "receives money from a customer and then, ***for a fee paid by the customer***, transmits that money to a recipient." *Velastegui*, 199 F.3d at 592 (emphasis added); *see also Banki*, 685 F.3d at 114 (adopting same definition of money transmitting business). It is undisputed that Tornado Cash did not charge a fee per transaction (and neither did Mr. Storm or the Peppersec developers).

The government acknowledges this but points out that relayers did charge fees. (Opp. at 36.) But the government fails to mention that using a relayer was optional and not essential to the Tornado Cash tool. (See *id.*) Moreover, the third-party relayers did not always charge a fee. (Ind. ¶ 24.) Even to the extent the relayers did charge a fee, their services were separate and distinct from the provision of software tools by Peppersec. That this optional service was made available to users did not transform Tornado Cash into a money transmitting business.

3. Adopting the Government's Expansive Definition of Money Transmitting Would Have Absurd and Adverse Consequences

The government tries to downplay the significance of this case by suggesting that the issue before the Court is not whether "cryptocurrency mixing services themselves are illegal,"

but rather whether anonymizing protocols must comply with FinCEN, KYC, and AML requirements. (Opp. at 31.) But as the Blockchain Association explained, compliance with the Bank Secrecy Act would be impossible for developers of anonymizing protocols, so adoption of the government's theory is tantamount to a ban on this technology. (BA Amicus Br. at 18.)

In fact, this issue is of such significance that two members of the United States Senate recently wrote to the Attorney General, asking him to reevaluate the Department of Justice's position sweeping non-custodial crypto software services into the definition of money transmitters. (*See* Exhibit A (Letter from Senators Lummis (R-Wyoming) and Wyden (D-Oregon) to Attorney General Merrick Garland (May 9, 2024)).) The bipartisan letter makes clear that the government's interpretation "contradicts the clear intent of Congress and the authoritative guidance of the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN)." (*Id.* at 1.) Specifically, the Senators explain that "[c]ustody and control are … the logical touchstone of where 'acceptance' and 'transmission' occurs on Bitcoin or other crypto networks." (*Id.* at 2-3.) The Senators also note the important congressional objective of "nurturing the development of transformative technologies." (*Id.* at 3.)

The government contends it would be arbitrary to have money transmitter liability turn on whether the Tornado Cash UI preserved the secret note. (Opp. at 30.) But the secret note is the key to control, so whether a developer has access to the secret note is exactly what money transmitter liability *should* turn on. Indeed, it would be absurd to impose criminal liability on a developer who has no ability to access or control the funds and, in fact, as here, has no ability to modify the software that was created or to control how or by whom it is used.

Finally, the government suggests that it can impose money transmitter liability against Mr. Storm and those like him because other punitive measures, *e.g.*, sanctioning wallets

associated with known money launderers, have practical limitations. (Opp. at 31 n.9.) But the fact that other punitive measures are imperfect does not give the government license to distort the money transmitter laws beyond recognition. Congress had good reason not to give the Department of Justice the broad authority it seeks. To do so would potentially drive software protocols aimed at protecting privacy out of existence and would chill the development of new software and other technologies. (*See* BA Amicus Br. at 17-20; Ex. A.) None of these adverse consequences is warranted because the proper statutory interpretation excludes anonymizing protocols such as Tornado Cash from the definition of money transmitters.

B. Count One, the Money Laundering Conspiracy Charge, Should Be Dismissed

The government has not alleged basic elements of concealment money laundering—namely, a financial transaction, a criminal agreement, and specific intent. Here, it was the perpetrators of the alleged hacks—not Mr. Storm and the Peppersec developers—who, according to the Indictment, engaged in the allegedly unlawful financial transactions. The government's concession that the Indictment fails to allege an agreement between these alleged bad actors and the Peppersec developers thus fatally undermines not only the illegal agreement and specific intent elements, but also the financial transaction prong, as the Indictment fails to allege that Mr. Storm and the Peppersec developers agreed to conduct the alleged transactions, knowing that such transactions involved the proceeds of specified unlawful activity. Ultimately, the government's opposition makes clear that the only agreement it can prove involving Mr. Storm was one to develop an agnostic software protocol, the creation of which is not money laundering.

1. The Indictment Does Not Allege That Roman Storm or Any Alleged Co-Conspirator Conducted a "Financial Transaction"

The government cannot show that Mr. Storm or his alleged co-conspirators "conducted" a "financial transaction" "involving the use of a financial institution," 18 U.S.C. §§ 1956 (a),

(c)(2), (c)(3), (c)(4)(B), because the Tornado Cash protocol is not a financial institution. The government admits that, to the extent its concealment money laundering theory rests on a financial transaction involving a financial institution, this element is not met if the Court dismisses Count Two. (*See* Opp. at 37.)

The government claims that Count One can survive even if Count Two is dismissed, however, because it charged not only a "financial transaction" "involving a financial institution" under subsection (c)(4)(B), but also a "financial transaction" meaning a "transaction" "affect[ing] interstate commerce" under subsection (c)(4)(A). (Opp. at 37-38.) This is not clear from the Indictment, given that subsection (c)(4)(B) contains additional elements that are not alleged, specifically that such transaction must involve the movement of funds by wire, involve monetary instruments, or involve the transfer of title to real property, vehicle, vessel or aircraft. 18 U.S.C. §§ 1956(c)(4)(A)(i)-(iii). Further gaps remain because, to amount to a "transaction" under Section 1956(c)(3), there must be a "purchase, sale, loan, pledge, gift, transfer, delivery or other disposition" of property, (*id.*; 3 Modern Jury Instruction Criminal P. 50-A-8), and the government failed to allege which one applies. Even if this Court presumes that the government would (but did not) allege that the "transaction(s)" at issue involved a "transfer" of "funds by wire," this does not provide the notice required by the Second Circuit. *United States v. Pirro*, 212 F.3d 86, 92 (2d Cir. 2000).

In any event, the problem with the alternative definition of financial transaction is not merely a matter of missing charging language. As to both definitions, the defendant must have conducted, or conspired to conduct, such transaction "knowing that the property involved" in such transaction "represent[ed] the proceeds of unlawful activity," namely, the proceeds of computer fraud and abuse or wire fraud. But the Indictment lacks a single allegation of a wire

(or crypto) transfer that Mr. Storm or the Peppersec developers (the alleged co-conspirators) conspired to conduct knowing that the property involved in that transfer "represent[ed] the proceeds of unlawful activity," namely the proceeds of computer fraud and abuse or wire fraud.

"The federal money laundering statute, [Section] 1956, prohibits specified transfers of money derived from unlawful activities." *Regalado Cuellar v. United States*, 553 U.S. 550, 557 (2008). The "financial transaction" requirement is specific and concrete. *See United States v. Leslie*, 103 F.3d 1093, 1101 (2d Cir. 1997) ($750,000 cash-for-checks exchange was a financial transaction); *United States v. Napoli*, 54 F.3d 63, 67 (2d Cir. 1995) (negotiation of fraudulent checks a financial transaction). The Indictment lacks a single alleged "financial transaction" conducted by Mr. Storm and the Peppersec developers. The only allegations of transactions involving the proceeds of unlawful activity are the transfers of cryptocurrency into the Tornado Cash protocol by third-party bad actors (*see* Dkt. 1, Indictment ("Ind.") ¶¶ 47, 48, 58, 68), none of whom is alleged to be a co-conspirator (*see* Opp. at 40). These allegations themselves make clear that none of the Peppersec developers conducted those transactions, much less did so knowing that they contained the proceeds of specified unlawful activity.[13]

2. The Indictment Fails to Allege the Existence of a Criminal Agreement to Launder Money

Conspiracy "'is the agreement . . . to commit one or more unlawful acts.'" *United States v. Jones*, 482 F. 3d 60, 72 (2d Cir. 2006) (quoting *Braverman v. United States*, 317 U.S. 49, 53

[13] This is true even if a bad actor used the Tornado Cash UI (although the Indictment lacks any allegation that they did), for several reasons: (1) the UI did not touch a user's cryptocurrency, and thus did not conduct a financial transaction between the user and the protocol; and (2) the UI had no way of knowing whether any particular transaction between a user and the protocol contained specified unlawful activity proceeds (and certainly the Peppersec developers did not). Similarly, relayers did not control any cryptocurrency withdrawal, so they did not conduct financial transactions and, in any event, they did not know whether any particular withdrawal contained the proceeds of specified unlawful activity.

(1942)). The basic element of a criminal agreement requires either an explicit agreement or an implicit agreement manifested through mutual interdependence of the alleged co-conspirators. *See United States v. Maldonado-Rivera*, 922 F.2d 934, 963 (2d Cir. 1990). The government agrees it must prove "that two or more people agreed to violate the money laundering statute, and that the defendant knowingly engaged in the conspiracy with the specific intent to commit the offenses that are the object of the conspiracy." (Opp. at 30 (citing *United States v. Garcia*, 587 F.3d 509, 515 (2d Cir. 2009); *see* MTD at 27 (same).)

The Indictment fails to allege facts that could show an illegal agreement; instead, the government intentionally conflates the agreement to develop the Tornado Cash protocol and UI with a (non-existent) later-in-time agreement to engage in purported concealment money laundering, based on nothing more than the allegation that some (unidentified) third-party bad actors used the "Tornado Cash service" for illicit purposes. Without an agreement between the bad actors and the Peppersec developers, the government cannot show a "meeting of the minds" as to the illegal objective of money laundering.

In response, the government disclaims any requirement to prove that Mr. Storm "reached a criminal agreement with those engaged in the underlying specified unlawful activity[,]" and attempts to rely instead only on a conspiracy between Mr. Storm and "at least Semenov and [Pertsev.]" (Opp. at 40.)[14] But this does not solve the problems with the Indictment's

[14] The government also raises and knocks down two irrelevant "straw men" arguments: (1) that the government is not required to prove an agreement to commit the alleged predicate offenses, and (2) that the government is not required to prove that Mr. Storm had knowledge of the specified unlawful activity. (Opp. at 40, 42). Neither of these points is in dispute, so there is no tension with *United States v. Stavroulakis*, 952 F.2d 686, 690 (2d Cir. 1992), or *United States v. Gamez*, 1 F. Supp. 2d 176, 181 (E.D.N.Y. 1998). *United States v. Sterlingov* is simply inapposite; the allegations there include defendant's alleged efforts to avoid detection by law enforcement, 573 F. Supp. 3d 28, 30-34 (D.D.C. 2021), which the government admits Mr. Storm

conspiracy theory: whether or not an express agreement is required, the government must show "sufficient proof of mutual dependence and assistance" between the perpetrators of the underlying criminal acts and the alleged money laundering conspirators (*see* MTD at 28-29 (collecting cases)), particularly where, as here, the same bad actors are alleged to have both perpetrated the underlying specified unlawful activity and to have conducted the financial transactions in which the proceeds of that activity were laundered.

The government fails to cite a single case where a conspiracy to commit money laundering charge was sustained without at least an implicit agreement between the perpetrator of the underlying crime and the defendant. To the contrary, the government's own cases help illustrate why such a connection is necessary. *Stavroulakis* involved a money laundering conspiracy in which the defendant was approached by "an undercover FBI agent … who said he was connected with organized-crime figures eager to launder substantial amounts of cash derived from narcotics transactions." *Stavroulakis*, 952 F.2d at 688. The defendants then conspired to engage in certain transactions to launder what they believed, based on the representations of the agent, to be ill-gotten gains. *Maher* involved a money laundering conspiracy in which defendants worked and communicated directly with a "large-scale heroin dealer," known by the codename "Joe," to launder drug money. *United States v. Maher*, 108 F.3d 1513, 1518, 1528 (2d Cir. 1997). In both cases, the intermediary (the agent or Joe) provided a link in the chain between the perpetrator of the underlying crime and the defendant accused of money laundering. Here, by contrast, the government tries to allege conspiracy without an agent or a Joe providing that link between the alleged perpetrators and the alleged money laundering co-conspirators.

---

did not do (in fact, he cooperated), as well as profiting directly from fees charged per transaction, *id.* at 33.

Contrary to the government's claim, the alleged agreement between Mr. Storm and the Peppersec developers is not sufficient to meet the element of an "illegal agreement" on its own. Indeed, when it finally gets down to summarizing the Indictment's factual allegations that it contends support a criminal meeting of the minds, the government argues that the Peppersec developers: (i) created the Protocol; (ii) paid to host the UI's website; (iii) paid for traffic between the UI and the blockchain; (iv) maintained "the relayer network"; (v) refused to implement AML programs; and (vi) deployed new features such as the relayer algorithm. (Opp. at 43.) Even accepting all these allegations as true—and they are not—these alleged facts are consistent with the day-to-day actions of software developers and a far cry from conduct sufficient to support an agreement to violate the anti-money laundering statute.

3. There Are No Allegations in the Indictment That Would Support a Specific Intent to Further an Illegal Purpose

Finally, the Indictment's allegations fail to meet the element of specific intent. While agreeing that "mere negligence would not amount to a Section 1956 violation," (Opp. at 44), the government fails to engage Mr. Storm's main argument: that the government seeks to convict him on the theory that he and the Peppersec developers did not implement KYC/AML into the UI and, therefore, should bear criminal responsibility for the actions of Tornado Cash users. (MTD at 30.) There is no dispute that the alleged underlying crimes were committed by third parties ***after*** Tornado Cash was already developed, launched, immutable, and publicly available on the Internet. (*Id.* at 31; Opp. at 43.) The timing alone undermines any inference of specific intent.

The government falls back on the bare "willfully and knowingly" charging language in the Indictment, arguing that it alone is sufficient to support the intent element. (Opp. at 44.)[15] To the contrary, that the government's own allegations demonstrate a lack of intent and, consequently, that the money laundering charge "fails to allege a crime within the terms of the applicable statute" is an appropriate basis for dismissal. *United States v. Aleynikov*, 676 F.3d 71, 75-76 (2d Cir. 2012). This failure is evident from the government's summary of Mr. Storm's alleged conduct (Opp. at 43), which is bereft of any allegation that he developed Tornado Cash with the intent to launder money or that he subsequently intended to commit money laundering. This grab bag of negligence-based accusations simply does not add up to specific intent.[16]

Next, the government fails to address Mr. Storm's argument that it has alleged only that he failed to take affirmative steps to try to block bad actors from engaging in bad conduct, which does not establish an intent to further or assist in that conduct. (MTD at 34-35.) The government attempts to make facile distinctions of the *Twitter* and *Risley* decisions (Opp. at 45-46), but it misunderstands their import: both stand for the proposition that the government's allegations of potential "profits" deriving from Tornado Cash are insufficient to demonstrate specific intent. *See Twitter, Inc. v. Taamneh*, 598 U.S. 471, 449-501 (2023); *Risley v. Universal Navigation Inc.*, 22 Civ. 2780 (KPF), 2023 WL 5609200, at *14 (S.D.N.Y. Aug. 29, 2023). Nowhere does the government dispute this point; nor does it matter that these are civil cases,

---

[15] The government cites *United States v. Percoco*, No. 16 Cr. 776 (VEC), 2017 WL 6314146, at *7 (S.D.N.Y. Dec. 11, 2017); *United States v. Light*, No. 00 Cr. 417, 2000 WL 875846, at *2 (N.D. Ill. June 29, 2000); both reject an argument that the government had to present its evidence of intent at the motion to dismiss stage. Mr. Storm does not make that argument here.

[16] As noted in the MTD, this is not the standard in the Netherlands, where an individual can be criminally liable for money laundering on a negligence theory. (MTD at 14, n.15.) On May 14, 2024, under that standard, Peppersec co-developer Alexey Pertsev was convicted of money laundering in the Netherlands. The defense understands that Mr. Pertsev plans to appeal his conviction.

since the specific intent standard of Section 1956 is more exacting than standards for the claims in those cases. *See Twitter*, 598 U.S. at 490 ("some culpable conduct is needed"); *Risley*, 2023 WL 5609200, at *14 (discussing Section 29(b) of the Exchange Act).

Finally, the government baldly asserts that the money laundering charge in this case is analogous to the charges in the *Silk Road* and *Bitcoin Fog* cases. (Opp. at 46.) The only similarity to those cases is the involvement of cryptocurrency, which, in the government's apparent view, is enough to be prosecuted. But unlike those cases, there is no allegation that Mr. Storm:

(i) expressed a desire to help criminals avoid law enforcement; (ii) concealed his alleged role in the protocol; (iii) tried to deceive the government or impede their investigation; (iv) had an arrangement to be compensated by criminals; or (v) did business or even communicated with sanctioned persons or entities. Without such allegations, and without the other critical allegations discussed above, Count One is fatally deficient and must be dismissed.

C. Count Three, the IEEPA Conspiracy Charge, Should Be Dismissed

The government primarily advances two flawed arguments in support of Count Three. First, it argues that the Tornado Cash protocol is not protected by the IEEPA's informational materials exemption because the so-called "Software and Technology Regulation" purportedly overrides the longstanding protections mandated by the First Amendment and expanded by the Berman Amendment. (*See* Opp. at 50-54.) Second, it argues that the "willfulness" of Mr. Storm's alleged IEEPA violation is established because he purportedly "deliberately chose an ineffective remedy" when Tornado Cash was allegedly misused by the Lazarus Group. No court

has ever approved either of the government's misguided theories.[17] (Opp. at 60.) This Court should not be the first to indulge this unconstitutional prosecutorial overreach.

1. Despite Government Claims to the Contrary, OFAC's Regulation of "Data Transmission" Software Does Not Apply

The government does not dispute that the First Amendment protects software under Second Circuit precedent, that the Berman Amendment sought to expand those protections, and that Congress expanded the scope of the Berman Amendment (*i.e.*, the informational materials exemption) in 1994 out of concern that the government had "narrowly and restrictively interpreted the language in ways not originally intended." (MTD at 37 (quoting H.R. Conf. Rep. No. 103–482, at 239, 1994 WL 151669 (1994)).) In fact, Congress acted because it disapproved of OFAC's attempt to impermissibly carve out "intangible materials" from the definition of "informational materials." *See United States v. Amirnazmi*, 645 F.3d 564, 585 (3d Cir. 2011).

Nevertheless, the government disingenuously tries to carve out software from the definition of "informational materials" because that word is not in the list of examples Congress provided in 1994. (*See* Opp. at 53-54 (citing 31 C.F.R. § 510.213(c)(3)).) Congress's exemplary and nonexclusive list is an expansion, not a limitation, of protections for informational materials "regardless of format or medium of transmission." 50 U.S.C. § 1702(b)(3); *see also Kalantari v. NITV, Inc*., 352 F.3d 1202, 1204-05 (9th Cir. 2003) (Congress "expanded the exemption's nonexclusive list of informational materials to include new media, such as compact discs and CD ROMs … in any '*format or medium of transmission*'") (emphasis added).

In an attempt to manufacture support, the government also misconstrues *Bernstein v. U.S. Dept. of State*, 974 F. Supp. 1288, 1308 (N.D. Cal. 1997), which actually found software

[17] *See, e.g.*, Dkt. 39-1, Amicus Br. of the DeFi Education Fund, Ex. A (chart of cases showing that the IEEPA has never been used to penalize a software developer under like circumstances).

regulation to be *invalid and unconstitutional* under the First Amendment. Moreover, the government deliberately ignores the fact that Congress's 1994 list does include CD-ROMs, which were used well before 1994 to store software.[18] It strains credulity to suggest that Congress intended to protect CD-ROMs (the actual physical object) but not their contents.

The government's reliance on OFAC's regulation is misplaced because it only applies to software used for "transmission of any data." 31 C.F.R. § 510.213(c)(3). The government repeatedly alleges Tornado Cash was used for "money transmission," not "data transmission." (Ind. ¶¶ 16, 32, 33, 79-82.) The government's overbroad view of "data transmission" threatens to create an all-encompassing software exception that will swallow the Constitutional and statutory rule of protection for informational materials. *See Federal Election Commission v. Political Contributions Data, Inc.*, 943 F.2d 190, 191 (2d Cir. 1991) ("we are obliged to construe statutes to avoid constitutional problems whenever possible").

2. The Informational Materials Exemption Defeats the IEEPA Conspiracy Charge

The government next argues it is not charging Mr. Storm for exporting software. (Opp. at 50, 55.) But it admits, as it must, that the charge is based on the alleged actions of hosting a website (which is code), maintaining the UI (also code), and developing the relayer algorithm (also code), as well as making public statements (not code, but plainly protected speech). (Opp. at 51.) At a minimum, this is indirect regulation of informational materials by using the IEEPA to reduce or eliminate use of software, *i.e.*, Tornado Cash. *See* 50 U.S.C. § 1702(b)(3) (forbidding regulation or prohibition "directly or indirectly"); *see also TikTok Inc. v. Trump*, 490

[18] *See* Shapiro *et al.*, *The Invention of Compact Discs*, Dartmouth (Nov. 9, 2012), available at https://bit.ly/3K0AjMg ("Launched in 1985 … the CD-ROM stores computer software and data.").

F. Supp. 3d 73, 81 (D.D.C. 2020); *Marland v. Trump*, 498 F. Supp. 3d 624, 637 (E.D. Pa. 2020) (finding indirect regulation by undermining app's functionality and preventing use).[19]

The government's primary attack on Mr. Storm—that he allegedly "chose an ineffective remedy"—also confirms that Mr. Storm is being prosecuted under the IEEPA for developing and publishing Tornado Cash code. (*See* Opp. at 60.) This is regulation of code by threat of enforcement, which violates the informational materials exemption. *See* 50 U.S.C. § 1702(b)(3).

The government's example of a financial institution using software to process transactions proves the point. (*See* Opp. at 55.) If a financial institution entered into a conspiracy to launder money for Lazarus Group, ***that institution*** would invite criminal liability, ***not the developer*** of the software used by the institution.[20] The government's nonsensical argument about the IEEPA's statutory context (Opp. at 56) does not override the plain statutory language or the expressed intent to afford broad protection to informational materials. *Amirnazmi*, 645 F.3d at 585 (informational materials exemption has "a broad scope."). This protection is not a "loophole" (Opp. at 57); it is exactly what Congress mandated.

This Court should be very concerned about the government's attempt to hold software developers criminally liable under federal sanctions laws for developing and exporting code. *See Risley*, 2023 WL 5609200, at*9 n.8 (expressing same concern with federal securities laws).

---

[19] The government tries to distinguish the TikTok cases because they involve a more robust "exchange of information" on social media. (Opp. at 68.) But the informational materials exemption protects *all* such materials, not just the ones the government deems worthy of protection. Moreover, the government concedes that American citizens who have used Tornado Cash have a legitimate privacy interest in protecting their information. (*Id.* at 58.)

[20] The government wrongly attacks *amicus curiae* Coin Center's analogy to SWIFT. (Opp. at 55 n.16.) It is unsurprising that SWIFT says it complies with ***applicable*** sanctions laws. The point is that SWIFT thinks U.S. sanctions laws may apply to its users but not to it because it is essentially a messaging services provider, and the government does not disagree. (*See* Dkt. 43, Amicus Br. of Coin Center at 16-17.)

Eschewing logic in favor of scare tactics, the government ominously portends that American banks will begin serving North Korea if Mr. Storm cannot be prosecuted under the IEEPA. (*See* Opp. at 57.) The real concern for society is the government's observation that software "touches nearly everything" (Opp. at 57), which is precisely why it is so dangerous to expand criminal liability to software developers because of alleged misuse of that software by others.

3. The Indictment Fails to Allege That Roman Storm Willfully Conspired to Evade Sanctions on North Korea

Even if the government could overcome the informational materials exemption, it still must prove that Mr. Storm willfully conspired to evade sanctions. (*See* MTD at 40-42.) The government concedes that the willfulness inquiry must be satisfied "at the time [Defendants] joined in a plan to engage in the unlawful acts." *See United States v. Quinn*, 403 F. Supp. 2d 57, 60 (D.D.C. 2005). But the date the conspiracy allegedly began is almost two years after Tornado Cash had become publicly available and immutable. (Ind. ¶ 26; Opp. at 59.) Thus, the sanctions evasion charges are essentially based on a post-hoc negligence theory. (*See* Ind. ¶¶ 9, 10, 29.) The government appears to be arguing that Mr. Storm had some duty to stop the Lazarus Group's alleged after-the-fact misuse of Tornado Cash. (Opp. at 60.) This novel argument is deficient for at least three reasons.

First, although the government claims Mr. Storm "could have done something," it nowhere explains what he could have done. (*See* Opp. at 60.) This is because there was no effective remedy. The government does not dispute the defense's position that the Tornado Cash code could not be changed or taken down and that the Lazarus Group was sophisticated enough to use it without any help from Mr. Storm, the UI, or the website, nor does it dispute that the government also took no steps to demand that the UI be taken down. (*See* MTD at 43-44.)

Second, the government tacitly concedes the lack of willfulness by failing to identify any deliberate choice to help the Lazarus Group allegedly evade sanctions. (*See* Opp. at 15, 47, 51, 60.) The government does not say it will prove that: (i) Mr. Storm had an agreement with the Lazarus Group to evade sanctions; (ii) the Lazarus Group paid him for his help (either directly or through a relayer); or (iii) the Lazarus Group used the UI or the website. The government has failed to allege the offense of conspiracy to violate the IEEPA.

Third, the government ignores the weight of the IEEPA cases establishing the lack of an IEEPA violation here. (*See* MTD at 44-45.) For example, Mr. Storm did not express a desire to help the Lazarus Group, and he even blocked the known Lazarus Group wallet address. (*See* Opp. at 61.) The Indictment does not allege that Mr. Storm tried to conceal the Lazarus Group's purported misconduct or deceive the government, that he made arrangements to be compensated by the Lazarus Group, or that he even communicated with the Lazarus Group or any other sanctioned entity. Although the government repeatedly alleges he "profited" from Tornado Cash, the Indictment does not allege any expectation of financial gain from Lazarus Group's allegedly illicit transactions. *See Risley*, 2023 WL 5609200, at *19 (rejecting contention that collecting transaction fees and hoping to profit from increased token values supported "a claim that [d]efendants had a financial interest in the particular transactions").

The government's theory in the Indictment is one of first impression: that a software developer can be held responsible for a third-party sanctioned entity's unsolicited use of their software. This theory is not supported by case law, and the government ignores the weight of the contrary caselaw cited by amici. For all these reasons, Count Three is legally deficient and must be dismissed.

D. All Counts Should Be Dismissed on First Amendment Grounds

1. The Statutes Are Facially Overbroad

As the government concedes, the First Amendment protects expression in the form of software and computer code. (*See* Opp. at 66-67; *see also Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 449-50 (2d Cir. 2001).) According to the government, all three statutes at issue proscribe the dissemination of constitutionally protected expression[21]—writing immutable code, hosting a website, maintaining the UI, developing the relayer algorithm, and making public statements. (Opp. at 63-65.) Assuming the government's interpretation of the statutes underlying the conspiracy charges is correct, the statutes prohibit a substantial amount of protected expression relative to their legitimate sweep and are thus overbroad. *See United States v. Williams*, 553 U.S. 285, 292 (2008).

Contrary to the government's claim, the statutes at issue here, as the government interprets them, impose a substantial burden on the constitutional rights of computer programmers. (*See* Opp. at 64.) On a facial challenge, the concern is whether "the threat of enforcement of an overbroad law deters people from engaging in constitutionally protected speech." *Williams*, 553 U.S. at 292. As the government's theory reveals, the statutes have a substantial chilling effect on the First Amendment rights of computer programmers who seek to improve privacy over financial transactions—itself a constitutionally protected interest, *Statharos v. N.Y. City Taxi & Limousine Commission*, 198 F.3d 317, 322-23 (2d Cir. 1999)—and

[21] By contrast, *United States v. Awan* (Opp. at 64) is inapposite because that statute, Section 1956(a)(2)(A), "simply prohibit[ed] the act of transporting funds across U.S. borders with the intent of promoting specified criminal activities" and thus had "no apparent impact on free expression." 459 F. Supp. 2d 167, 183 (E.D.N.Y. 2006), *aff'd*, 384 F. App'x 9 (2d Cir. 2010).

the effect will only continue to grow as the technology proliferates. (*See* MTD at 48; *see also* Ex. A (U.S. Senators expressing concerns about chilling effect of DOJ's prosecutions).)

2. The Statutes Violate the First Amendment As Applied

Even if the statutes were not facially overbroad, they cannot survive First Amendment scrutiny as applied. The regulations at issue here, as applied, are content-based and trigger strict scrutiny. If a law cannot be "justified without reference to the content of the regulated speech" or was "adopted by the government 'because of disagreement with the message [the speech] conveys,'" it is content-based. *Reed v. Town of Gilbert, Ariz.*, 576 U.S. 155, 163-64 (2015) (quoting *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989)); *see also Corley*, 273 F.3d at 451-52.

The Indictment targets the Tornado Cash suite of software code not for its functional capability but for the message it conveys—the promotion of privacy.[22] (*See, e.g.*, Ind. ¶ 11 (citing Mr. Storm's presentation explaining that Tornado Cash "improves transaction privacy" and "ensur[es] complete privacy"); *id.* ¶ 21 (citing Mr. Storm's interview statements regarding privacy).) As such, the regulations are content-based and subject to strict scrutiny, meaning they are "presumptively unconstitutional and may be justified only if the government proves that they are narrowly tailored to serve compelling state interests." *Reed*, 576 U.S. at 163.

Even if the regulations were, as applied, content-neutral and thus subject to intermediate scrutiny, the government cannot meet its burden of proving its regulations withstand First

[22] The government's reliance on *CFTC v. Vartuli*, 228 F.3d 94, 109-12 (2d Cir. 2000), is thus misplaced, as the court there held that an automated trading system was not protected speech, but notably it also held that an injunction against publishing the underlying software itself may constitute a prior restraint on protected speech. The government's contention that the First Amendment is not implicated "where the software was allegedly used for criminal purposes" is also unsupported, as the cases cited in support involved the defendants' publication of *malware*, not software with legitimate privacy-enhancing uses. (*See* Opp. at 66.)

Amendment scrutiny, *see Edenfield v. Fane*, 507 U.S. 761, 770 (1993), because the regulations "burden substantially more speech than is necessary," and there are less restrictive means to achieve its goals. *Corley*, 273 F.3d at 454. (*See also* MTD at 50-51.) Most obviously, the government could require an actual money transmitting business to collect from any user documentation proving the source of such funds—which, as the Indictment acknowledges, the Tornado Cash Compliance Tool allows any user to generate. (Ind. ¶ 39.)

E. All Counts Should Be Dismissed on Due Process Grounds

1. The Statutes Are Unconstitutionally Vague

The three statutes underlying the conspiracy charges are vague on their face and as applied. The government begins by erroneously contending that the Court should first determine whether the statutes are vague as applied to Mr. Storm's conduct and, if not, not even consider a facial vagueness challenge. (*See* Opp. at 69-70 quoting *United States v. Requena*, 980 F.3d 30, 39 (2d Cir. 2020).) The government ignores a key distinction in *Requena*: where "the statute implicates rights protected by the First Amendment," a defendant "may raise a facial challenge" regardless of whether the statute is vague as applied. 980 F.3d at 39. This is because "vagueness in the law is particularly troubling when First Amendment rights are involved." *Farrell v. Burke*, 449 F.3d 470, 485 (2d Cir. 2006). Here, the statutes implicate the First Amendment right to expression, and the Court may consider the vagueness of the underlying statutes both as applied and in "other, hypothetical applications of the statute[s]." *Id.* at 494.

In arguing that the statutes here are not vague, the government impermissibly focuses on the language of the Indictment rather than on the language of the statutes. (*See* Opp. at 71-73.) "[A]ll vagueness challenges—whether facial or as-applied—require [the court] to answer two separate questions: whether *the statute* gives adequate notice, and whether it creates a threat of

arbitrary enforcement." *Id.* (emphasis added). And it makes sense, as it would serve no purpose if a defendant is provided notice or "fair warning" of what conduct is criminalized only after being indicted. *See United States v. Lanier*, 520 U.S. 259, 266 (1997).

The *statutes* underlying the three conspiracy charges here—as interpreted by the government—"fail[] to provide a person of ordinary intelligence fair notice of what is prohibited" and "authorize[] or encourage[] seriously discriminatory enforcement." *Williams*, 553 U.S. at 304. This is especially true under the heightened standard that applies to criminal statutes that also "might infringe constitutional rights." *See Rubin v. Garvin*, 544 F.3d 461, 467 (2d Cir. 2008). All three counts attempt to criminalize the publication of computer software code and the maintenance of a website. A person of ordinary intelligence cannot, from the language of the statutes, draw the line between conduct that is permitted and criminalized.

2. The Rule of Lenity Requires Dismissal

All three counts should also be dismissed based on the rule of lenity. The government contends that the statutes are not ambiguous and that the rule does not apply where the "best reading of the statute extends to his conduct." (Opp. at 76.) Mr. Storm agrees that the statutes are not ambiguous—they clearly do not apply to his alleged conduct, as set forth above. It is the government's strained interpretation of them that would create ambiguity. To the extent there is ambiguity whether these statutes apply to computer programmers not involved in the actual transactions that violate the underlying statutes, the rule of lenity should be applied to dismiss the Indictment.

3. The Indictment Impermissibly Relies on Novel Constructions of Criminal Statutes

All three counts should also be dismissed on due process grounds because they rely on a novel construction of criminal statutes. The government's argument that "[s]ome case has to be

first" misses the mark. (*See* Opp. at 77.) The charges here are not just the first application of longstanding statutes to new facts—they rely on a construction "that neither the statute[s] nor any prior judicial decision has *fairly* disclosed to be within its scope." *Lanier*, 520 U.S. at 266 (emphasis added). All three charges rely on a novel and unprecedented application of statutory language that is unsupported by implementing regulations and regulatory guidance and, as such, due process requires their dismissal.

III. CONCLUSION

For all the reasons above and in the motion to dismiss, the Court should dismiss all counts of the Indictment with prejudice.

Dated: May 24, 2024

Respectfully submitted,

/s/ Brian E. Klein

Brian E. Klein
Keri Curtis Axel
Kevin M. Casey
Waymaker LLP

Attorneys for Roman Storm